NSTISSD No. 500
25 February 1993

NSTISS

**NATIONAL
SECURITY
TELECOMMUNICATIONS
AND
INFORMATION
SYSTEMS
SECURITY**

INFORMATION SYSTEMS SECURITY (INFOSEC)

EDUCATION, TRAINING, AND AWARENESS

19990429 002

DTIC QUALITY INSPECTED 2

NSTISSC

**NATIONAL SECURITY
TELECOMMUNICATIONS
AND
INFORMATION SYSTEMS
SECURITY COMMITTEE**

CHAIRMAN

February 25, 1993

FOREWORD

1. A key responsibility assigned by the "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990, is to ensure the development and implementation of a comprehensive approach to protect U.S. Government national security information systems. The success of this program depends not only on the technical implementations of policies, but also on the integration of human interfaces with automated systems. Education, training, and awareness are countermeasures that effectively reduce exposure to a variety of known risks. In order to achieve this end, it is essential to have a federal work force that is aware of, and educated about, the problems of information systems security (INFOSEC). This directive is issued in response to the national policy and establishes the requirement for federal departments and agencies to develop and implement INFOSEC education, training and awareness programs. This directive supersedes NTISS Directive No. 500, "Telecommunications and Automated Information Systems Security Education, Training, and Awareness," dated 8 June 1987.

2. Representatives of the National Security Telecommunications and Information Systems Security Committee may obtain additional copies of this directive from:

> Executive Secretariat
> National Security Telecommunications and
>   Information Systems Security Committee
> National Security Agency
> 9800 Savage Road
> Fort George G. Meade, MD 20755-6000

3. U.S. Government contractors are to contact their appropriate government agency or Contracting Officer representative regarding distribution of this document.

CHARLES A. HAWKINS, JR.
Acting

INFORMATION SYSTEMS SECURITY (INFOSEC)

EDUCATION, TRAINING, AND AWARENESS

SECTION I - PURPOSE

1. This directive establishes the requirement for federal departments and agencies to develop and implement information systems security (INFOSEC) education, training and awareness programs for national security systems.

SECTION II - SCOPE AND APPLICABILITY

2. This directive is applicable to all departments and agencies of the U.S. Government, their employees, and contractors who develop, acquire, manage, or use information systems operated by or on behalf of the Federal Government to store, use, process, transmit, or communicate national security information.

SECTION III - AUTHORITY

3. This directive is issued pursuant to "National Policy for the Security of National Security Telecommunications and Information Systems," dated 5 July 1990, which mandates the development and implementation of a comprehensive approach to protect U.S. Government national security information systems.

IV - DEFINITIONS

4. Definitions for terminology used in this directive may be found in NSTISSI No. 4009, "National Information Systems Security (INFOSEC) Glossary," dated 5 June 1992.

SECTION V - RATIONALE AND OBJECTIVES

5. The evolution of information processing technologies has enabled the Federal Government to transmit, communicate, collect, process, and store unprecedented amounts of information. The use of information systems by the Federal Government has focused attention on the need to ensure that these assets (i.e., hardware, software, and processing capabilities) and the information they process are protected from actions that would jeopardize the ability of departments and agencies to effectively and accurately perform official functions. The responsibility for securing this information and the systems on which it is processed lies with the head of the federal department or agency to whom the information and resources are entrusted.

6. The objective of this directive is to require the implementation of programs to enhance awareness of all persons within these departments and agencies of the need to ensure the protection of information in systems, as well as systems resources and capabilities; to enhance the public's confidence in the Federal Government's ability to provide information systems protection; and to promote the protection of information systems at the national level through an education, training, and awareness program that promotes a uniform and consistent understanding of the principles and concepts of INFOSEC.

1

SECTION VI - INFOSEC EDUCATION, TRAINING, AND AWARENESS

7. INFOSEC education, training, and awareness activities are required for all employees. Such a comprehensive effort must meet the varying levels of knowledge, experience, and responsibilities of employees, as well as the specific needs of individual departments and agencies. There are certain messages that need to be conveyed:

   a. Organizations critically rely on information and information systems' resources.

   b. The organization, through its management, commits to protect information and information systems' resources.

   c. There are threats, vulnerabilities, and related risks associated with the organization's information systems.

   d. There are consequences from the lack of adequate protection of the organization's information systems' resources.

   e. The employee is the essential element of a successful protection program.

8. Every INFOSEC education, training, and awareness program will contain three types of activities: initial orientation, more advanced education and training commensurate with duties and responsibilities, and reinforcement activities.

9. All training activities pursuant to the requirements of this directive shall be conducted by individuals who are knowledgeable of INFOSEC principles and concepts, as well as their application.

SECTION VII - RESPONSIBILITIES

10. Each federal department and agency will:

   a. Develop, implement, and evaluate an INFOSEC education, training, and awareness program in accordance with the National Manager guidelines.

   b. Require contractors to comply with the provisions of this directive whenever they develop, acquire, manage, or use information systems operated by, or on behalf of, the Federal Government to store, use, process, or communicate national security information. For contractors, the terms of the contract shall specify this requirement.

   c. Consistent with applicable laws, security requirements, department and agency policy, and resource availability, make information copies of INFOSEC education, training, and awareness materials available to the National Manager in furtherance of the responsibility assigned in paragraph 11.c. below.

11. The National Manager will:

   a. Develop INFOSEC education, training and awareness program guidelines and provide these to federal departments and agencies, including federal contractors, as requested.

   b. Ensure that appropriate education, training, and awareness materials are developed on INFOSEC policies, standards, criteria, products, and technologies that result from federal or federally sponsored efforts.

c. Subject to the approval of the originating department or agency, and consistent with applicable laws and security requirements, collect and maintain information on INFOSEC education, training, and awareness programs. Make such information available to government departments, agencies, and federal contractors, as requested.

d. Develop and conduct, or assist other federal departments and agencies in developing and conducting, INFOSEC education, training, and awareness activities, as requested.

DISTRIBUTION:

  NSA
  NSC
  OMB (Intel Branch NSD)
  OASD (C3I/TS) (2)
  ODASD (CI & SCM)
  DODSI
  DA (SAIS-SDC) (15)
  CNO (OP941J) (3)
  CMC (CC) (5)
  COMJSOC (J62)
  The Joint Staff (J6K) (2)
  The Joint Staff (DIRM/SCD/ISOB)
  USCINCLANT (J6) (2)
  USCINCCENT (CCJ6) (4)
  USCINCEUR (ECJ6) (2)
  CINCFOR (FCJ6) (2)
  USCINCPAC (J6) (2)
  USCINCSO (SCJ6) (2)
  USCINCSPACE (J4-J6) (2)
  USCINCSOC (SOJ6) (2)
  USSTRATCOM (2)
  USCINCTRANS (TCJ6) (2)
  TIC/DSS (2)
  HQ USAF (SCXX) (3)
  HQ USAF (SCS) (3)
  AFCSC (SRMP) (10)
  AFCSC/SRVT
  COMUSFJAPAN (J6) (2)
  COMUSFKOREA (J6) (2)
  Defense Courier Service (2)
  DIA (DSE-2B) (10)
  DIR JITC
  DIS (V0432) (5)
  DIS (V0060)
  DLA (DLA-IA) (2)
  DNA (ISIS)
  CDR JIEO
  COMDT COGARD (G-TTS-4) (3)
  COMCOGARDLANTAREA
  COMCOGARDPACAREA
  COMCOGARDONE
  COMCOGARDTWO
  COMCOGARDFIVE
  COMCOGARDSEVEN

COMCOGARDEIGHT
COMCOGARDNINE
COMCOGARDELEVEN
COMCOGARDTHIRTEEN
COMCOGARDFOURTEEN
COMCOGARDSEVENTEEN
COMSPAWARSYSCOM (PMW 151) (3)
DCMS (TD) (2)
CG MCDEC (DEVCEN C3) (2)
Dept. of Agriculture (MSD/FAS) (2)
Dept. of Commerce (OIRM/TMD) (2)
Dept. of Energy (AD241.1) (2)
Dept. of Health & Human Services (IG) (2)
Dept. of Interior (PPS-S MS5040 MIB) (2)
Dept. of Justice (JMD/SEPS) (2)
Dept. of State (DS/CMI/ISS) (5)
Dept. of State (SA-34, DTS-PO)
Dept. of Transportation (OIS M-70) (2)
Dept. of Treasury (MST) (10)
CIA (OC-CSD) (2)
CIA (DIR OIT) (2)
CIA (ISSG/OS) (2)
CIA (Chief, TEMPEST Division, (OS) (2)
CIA (Chief INFOSEC OIT)
CIA (Reference Library)
DIR, CCISCMO (2)
DIR, CCISCMO (Planning Office) (2)
DISA (Code DIPP) (5)
DMA (TSC)
DMA (IS)
Drug Enforcement Administration (OSTC) (2)
FAA (ACO-300) (6)
FBI (TSD) (5)
FCC (OMD) (2)
FEMA (NP-IR) (7)
GSA (KVI) (6)
NASA (JIS)
NASA (OS) (2)
NASA (JT)
NCS (MGR) (2)
NRC (8203-MNBB) (3)
USDELMC (INFOSEC REP)
U.S. Customs Service (65)
WHCA

INTERNET DOCUMENT INFORMATION FORM

A . Report Title: INFORMATION SYSTEMS SECURITY (INFOSEC) EDUCATION, TRAINING, AND AWARENESS

DATE Report Downloaded From the Internet   APRIL 1999

C. Report's Point of Contact: (Name, Organization, Address, Office Symbol, & Ph # NATIONAL SECURITY TELECOMMUNICATIONS AND INFORMATION SYSTEMS SECURITY TOLL FREE 1-888 678 4772
D.

D. Currently Applicable Classification Level: Unclassified

E. Distribution Statement A: Approved for Public Release

F. The foregoing information was compiled and provided by:
 DTIC-OCA, Initials:__JC_ ____Preparation Date: 27 APR 1999

The foregoing information should exactly correspond to the Title, Report Number, and the Date on the accompanying report document. If there are mismatches, or other questions, contact the above OCA Representative for resolution.

bb.

U99-05-0367